Criminal Intelligence Collection and Maintenance

606.1 PURPOSE AND SCOPE

It is the policy of the Hayward Police Department to collect, process, maintain and, under proper circumstances, disseminate suspicious incidents and both developmental and criminal intelligence information on individuals, groups, associations and organizations who or which are: (1) subject of efforts to gather more information for legitimate law enforcement purposes or (2) reasonably suspected of definable criminal or terrorist activity. This effort is necessary to suppress criminal and/or terrorist activity and thereby provide for the safety and security of persons and property within the City of Hayward.

The purpose of this policy is to declare the intention of the Hayward Police Department to comply with the standards established by the California Attorney General Guidelines, Code of Federal Regulations, Title 28, Part 23 and the Law Enforcement Intelligence Unit (LEIU) Criminal Intelligence File Guidelines. These standards strike the proper balance between the needs of law enforcement to collect, apply and share intelligence in a manner that protects an individual's Constitutional rights and right of privacy.

606.1.1 ACCREDITATION STANDARDS

This section pertains to the following CALEA standards: 42.1.6, 82.3.5

606.2 CRIMINAL INVESTIGATION BUREAU

A function of the Criminal Investigation Bureau is to collect, process, maintain and disseminate suspicious incidents and information on individuals, groups, associations and organizations reasonably suspected of definable criminal activity in order to suppress such activity. It is the responsibility of all Departmental personnel to report any suspicious incidents or criminal intelligence relating to criminal or homeland security activities to the Information and Intelligence Bureau. The objectives are:

(a) To provide intelligence support for Patrol and Special Operations with an emphasis on officer safety; and

(b) To develop strategic intelligence assessments designed to:

1. Identify criminal organizations which engage in, facilitate or otherwise support criminal activity which impacts the City of Hayward ;
2. Identify individuals who engage in criminal activity which impacts the City of Hayward ;
3. Provide guidance on the best use of resources to provide for control of individual and organized criminal activity which impacts the City of Hayward ; and
4. Provide insights into emerging crime trends which may impact the of City of Hayward.

5. Collect, process and disseminate information related to suspicious incidents, which occur in/around the city limits.

(c) To enable the Department to cooperate with and participate in local, state and national intelligence initiatives which benefit the residents of the City of Hayward.

606.3 DEFINITIONS

Activity Which Endangers the Public: means any activity which is carried out on a scale which or in a manner which (or both) endangers the participants, any person observing or present during the activity or public or private property.

Criminal Activity: means any activity which violates federal statutes, state statutes, local ordinances or codes and is made a criminal act by such statutes, ordinances or codes.

Criminal Associate: means any person(s) who is reasonably suspected of knowingly supporting, assisting or facilitating criminal activity by a person(s), group, association or organization in any manner.

Criminal Intelligence File: means a file relating to a specific person, group, association or organization which contains criminal intelligence information that demonstrates a criminal predicate exists as to the person, group, association or organization. In this context "person" may include persons known to exist whose identities have not yet been ascertained.

Criminal Intelligence Information: means legally gathered factual data which has been analyzed to determine that it is relevant to the identification of or the criminal activity engaged in by person(s), groups, associations or organizations.

Criminal Intelligence System or Intelligence System: means the arrangements, equipment, facilities and procedures used for the gathering, analyzing, receipt, storage, access and dissemination of criminal intelligence information, criminal intelligence files, developmental information and developmental files, and the inter-jurisdictional pooling of the information contained in the individual agency files.

Criminal Predicate: means criminal intelligence information which supports the finding that there is reasonable suspicion to believe that a person(s), group, association or organization is engaged in definable criminal activity. This term is the standard by which the determination as to whether information may be used to create an intelligence file is made.

Developmental Information: means information about activity which endangers the public that is gathered for a legitimate law enforcement purpose.

Developmental (Temporary) File: means a file which contains developmental information on person(s), groups, associations or organizations which information is held and analyzed for a discrete period of time to determine whether a criminal predicate exists. Such files may also be known as "tips and leads", "working files" or "temporary files".

Legitimate Law Enforcement Purpose: means information about activity which endangers the public and is gathered by law enforcement to determine whether a criminal predicate exists which would support the creation of an intelligence file.

Need to Know: means a state of facts that supports the legitimacy of access to specific intelligence by a person with a right to know. The need to know must be pertinent to and necessary to the performance of a specific law enforcement activity.

Reasonable Suspicion: means the state of known information which establishes sufficient facts to give a trained law enforcement officer, criminal investigator or employee a basis to believe that a person(s), group, association or organization is engaged in definable criminal activity or enterprise.

Right to Know: means having the legal status that allows the party to have access to criminal intelligence information. 28 CFR § 28.20(e) imposes the qualification that the right to know must be in "the performance of a law enforcement activity." Such status may be based on status as a law enforcement officer, investigator or employee or may be based on a court order, statute or a binding judicial decision if there is a need to know.

606.4 COMMAND AND CONTROL

(a) The Chief of Police of the City of Hayward or the Criminal Investigation Bureau Lieutenant shall be responsible for supervising the intelligence system and ensuring that these policies and procedures are enforced.

(b) The Chief of Police shall meet with the Criminal Investigation Bureau Lieutenant at least once a month or whenever the circumstances require. The purpose of this meeting shall be to inform the Chief of Police of the activities of the Intelligence Bureau and obtain guidance on issues that require executive level guidance.

(c) The Criminal Investigation Bureau Lieutenant shall have overall responsibility for all aspects of the intelligence system, including the training of Departmental personnel and auditing of the system. This person shall also be responsible for reviewing files to determine whether they have source and content validity as well as determining whether the files are current. The training of Department personnel will be accomplished on an individual or group basis depending upon the needs of the Department and will cover this entire policy.

606.5 DEVELOPMENTAL (TEMPORARY) FILES

(a) Developmental files may be created and used for the sole purpose of gathering information to determine whether there is reasonable suspicion that person(s), groups, associations or organizations as to whom or which the information is gathered are engaged in definable criminal activity which would permit the creation of an intelligence file. An individual, organization, business or group may be given "temporary" status in the following cases:

1. Subject or entity is unidentifiable '" The subject or entity, although suspected of being engaged in criminal activities, has no known physical descriptors, identification numbers, or distinguishing characteristics available.
2. Involvement is questionable '" Involvement in criminal activities by a subject or entity is suspected which has either:
    (a) Possible criminal associations '" Individual, organization, business, or group not currently reported to be criminally active but associates with a known criminal who is reasonably suspected of being involved in illegal activities.
    (b) History of criminal conduct '" Individual, organization, business, or group not currently reported to be criminally active but has a history of criminal conduct; and the circumstances currently being reported (i.e., new position or ownership of a business) indicate they may have, again, become criminally active.
    (c) Reliability and/or validity unknown '" The reliability of the information sources and/or the validity of the information cannot be determined at the time of receipt; however, the information appears to be significant and merits temporary storage while verification attempts are made.
    (d) Developmental (Temporary) files shall be "actively" worked in an effort to determine whether it should be added to the intelligence files or be destroyed. Failure to actively work and document the files progress will be grounds for the file in question to be destroyed.

(b) Developmental files shall be permitted for legitimate law enforcement purposes only and shall be maintained for a period of time not to exceed one (1) year.

(c) Developmental files shall not include information regarding political, religious, sexual information or social views, associations or activities unless such views, associations or activities are directly related to the activity which is believed to be criminal and which is the basis for creating the developmental file.

(d) Information placed in developmental files shall be information collected using only legal methods. Any information offered from any source which is known to have been or learned to have been unlawfully obtained shall be rejected or purged.

(e) In no case shall Criminal Offender Record Information (CORI) or Department of Motor Vehicle (DMV) data be incorporated into the intelligence file (Title 11 CFR Section § 703). The CORI/DMV files shall be kept at a separate location from the intelligence file system.

(f) Developmental files shall be maintained in the same secure location as intelligence files, but shall not be commingled with intelligence files. Developmental files shall be subject to the same command and control requirements as intelligence files.

(g) Developmental files shall be assigned a discrete identifying number.

(h) The developmental file contents shall be governed by the same content evaluation rules as apply to intelligence files.

606.5.1 DISSEMINATION /ACCESS RULES FOR DEVELOPMENTAL FILES

(a) These files shall be accessed only on a need to know/ right to know basis.

(b) The Criminal Investigation Bureau Lieutenant shall determine who shall have access to these files.

(c) If access is granted by use of an intranet or internet connection with the authorized recipient that access shall be read only and no printing shall be permitted.

(d) If access is not remote it shall be granted in the secure area only and the file shall not be permitted to be removed from the secure area.

(e) Any printing or copying of developmental files or any portion of developmental files shall occur only if the Criminal Investigation Bureau Lieutenant approves. Both the request to print or copy and the approval shall be documented. The requesting party shall not be permitted to print or copy unless that party has demonstrated to the Hayward that that party has written policies and procedures in place which are at least as stringent as these policies and procedures. The requesting party shall agree in writing that it will not disseminate the developmental information received to a third party without notification to and consent from the Hayward.

(f) When a file is printed or copied the recipient party shall be given the discrete number assigned to that file.

(g) In all cases when there is an imminent threat of harm to persons or property, information in these files which might assist in preventing such harm shall be disseminated to persons, agencies or other entities, public or private who may be in such imminent danger or in a position to assist in preventing such harm.

606.5.2 PURGING OF DEVELOPMENTAL FILES RULES

(a) Developmental files shall be retained for no more than one year. If at the end of this period no criminal predicate has been established, or if the file contains inaccurate information, the file and all its contents shall be destroyed. Because of the requirements of Government Code Section § 26202 documents such as developmental files cannot be actually destroyed until two years after their creation. Therefore, a developmental file which does not become an intelligence file shall, at the end of the one year period:

1. Be removed from the developmental file system;
2. Be sealed;
3. Be signed by the person sealing the file; and
4. Be stored in a secure location until actual destruction. In such situations, the discrete file number shall be retained and the file shall be identified by that number only. The developmental file system shall carry the notation that the file, identified by the discrete number, has been removed from the system and sealed. When the actual destruction occurs, the notation shall be changed to reflect the destruction of the file.

(b) Any and all persons/agencies other than Hayward personnel who were given access to a developmental file shall be notified that no criminal predicate was established and that the file has been destroyed. Copies of these notices shall be maintained by the Hayward. These notices shall use the discrete number rather than the name of any person(s), group, association or organization.

(c) Any persons/agencies given permission to print or copy all or any portion of the developmental file shall be notified as required by item 2 above and shall also be asked to provide written (paper or electronic) verification that the information has been purged from their system. Copies of that verification shall be maintained by the Criminal Investigation Bureau.

(d) In all cases the documents attesting to the destruction of developmental files shall use the discrete number assigned to the file instead of any identifier which could be traced to any person(s), group, association or organization.

606.6 CRIMINAL INTELLIGENCE FILES

(a) Criminal intelligence files shall be created and maintained as to persons, groups, associations and/or organizations only when there is reasonable suspicion that the subject(s) is/are engaged in definable criminal activity. A criminal intelligence file is only useful if its information is reliable, accurate and current. The two critical components of information to determine these values are:

1. The reliability of the source.
2. The validity of the content.

(b) Criminal intelligence files shall be maintained for a time period not to exceed five years unless:

1. Before the five year period has elapsed it is discovered that the information upon which the determination that reasonable suspicion existed was inaccurate or illegally obtained. In such situations the information which was inaccurate or illegally obtained shall be purged from the file and the file shall be reevaluated to

determine whether the remaining information supports a finding of reasonable suspicion; if it does the edited file shall be retained, if it does not the entire file shall be destroyed.

2. Before the five year period has elapsed additional information that supports the initial reasonable suspicion determination or demonstrates an additional criminal predicate exists comes to the attention of the intelligence unit. In such cases, a new five year retention period shall start from the date of discovery of the additional information.

3. An intelligence file may be maintained for an indefinite period of time so long as there is information that demonstrates the continued validity of the criminal predicate or another criminal predicate within the last five years.

(c) Excluded Material: Only lawfully collected information, based on a reasonable suspicion of criminal activity, should be stored in criminal intelligence files. Information that shall be specifically excluded from criminal intelligence files includes:

1. Information on an individual or group merely on the basis that such individual or group supports unpopular causes.

2. Information on an individual or group merely on the basis of race, gender, age, sexual preference or ethnic background.

3. Information on an individual or group merely on the basis of religious or political affiliations or beliefs.

4. Information on an individual or group merely on the basis of personal habits and/or predilections that do not violate any criminal laws or threaten the safety of others.

5. Information on an individual or group merely on the basis of involvement in expressive activity that takes the form of non-violent civil disobedience that amounts, at most, to a misdemeanor offense.

6. In no case shall Criminal Offender Record Information (CORI) or Department of Motor Vehicle (DMV) data be incorporated into the intelligence file (Title 11 CFR § 703). The CORI/DMV file shall be kept at a separate location from the intelligence file system.

(d) Information contained in intelligence files shall be collected only using legal means. Any information offered from any source which is known to have been or is learned to have been illegally obtained shall be rejected or purged from the intelligence file(s).

(e) Intelligence files shall be maintained in a secure location which cannot be accessed by the public or agency personnel not assigned to the intelligence unit without the permission of the Criminal Investigation Bureau Lieutenant. Developmental files shall be maintained in the same secure location but separate from the intelligence files.

1. The secure area shall be physically separate from other areas.
2. All files shall be maintained under lock and key or, if electronic, password protected. File access shall be limited to personnel assigned to the Intelligence Bureau unless another law enforcement officer or law enforcement agency employee has been granted access pursuant to another provision of these policies.
3. A log of persons requesting intelligence information from the Intelligence Bureau, after stating their lawful purpose, shall be maintained on a daily basis and shall be available for audit.
4. Each file maintained by the Intelligence Bureau, either developmental file or intelligence file, shall have an access log attached to it. This log, whether in paper or electronic form, shall show who has accessed the file, the date of the access and the purpose for the access. These access rules and log requirements shall apply to persons assigned to the Intelligence Bureau as well as all other persons. This file log shall be maintained on a daily basis and shall be available for audit.

(f) Each intelligence file shall be assigned a discrete number.

(g) File contents rules:

1. Each file shall contain copies of the source documents which were the basis for the finding that reasonable suspicion (or a legitimate law enforcement purpose) existed.
2. When additional information is added to the file copies of source documents shall also be added.
3. Information placed in the file shall be labeled for source reliability and content validity prior to its submission for entry into the file. The Intelligence Bureau manager or his/her designee will be responsible for approving all information contained in the file. Certain combinations of information standing alone will not support a finding of reasonable suspicion. (Examples would be an unreliable source which has provided information the content validity of which could not be judged or was doubtful). If reasonable suspicion has already been established from appropriate sources, then addition of information from an unknown source that cannot be judged as to content validity might be appropriate. It is difficult to justify adding information from an unreliable source that has doubtful or cannot be judged content validity to an existing file regardless whether reasonable suspicion has already been established.
    (a) Source reliability is based on the accuracy and consistency of the information provided by a given source. The categories of source reliability are:

1. Reliable: The reliability of the source is unquestioned or has been tested in the past.
2. Usually reliable: The source of information can usually be relied upon. The majority of the information provided in the past has proved to be reliable.
3. Unreliable: The reliability of the source has been sporadic in the past.
4. Unknown: The reliability of the source cannot be judged; either experience or investigation has not yet determined authenticity or trustworthiness.

(b) Content validity is an assessment of the truthfulness of the information provided by the source. The categories of content validity are:

1. Confirmed: The information has been corroborated by an investigation or another reliable, independent source.
2. Probable: The information is consistent with past accounts or other information.
3. Doubtful: The information is inconsistent with past accounts or other information.
4. Cannot be Judged: The information cannot by judged as to its truthfulness because of lack of time to investigate it or its lack of relation to or corroboration by any other information.

(c) Re-evaluation of criminal intelligence should be an ongoing process and each file shall be continually re-evaluated by the assigned investigator. This process will re-evaluate and cull the information that has no potential to become intelligence matter from the rest of the information. The process will be dynamic and unique to each "batch" of information.

4. Each file shall contain the name of the person(s) who analyzed the information and a statement of the reasons on which that person(s) based his /her finding of reasonable suspicion (such reasons may include conclusions based on training or experience so long as the specific relevance of that training or experience is articulated).
5. Each file should describe the definable criminal activity of which the file subject is reasonably suspected (or articulate the public safety concern that underlies the legitimate law enforcement purpose). Examples would include the following:

(a) Narcotics Trafficking.

(b) Unlawful Gambling.

(c) Loan Sharking.

(d) Extortion.

(e) Vice and Pornography.

(f) Infiltration of Legitimate Business for Illegitimate Purpose.

(g) Bribery.

(h) Major Crimes Including Homicide, Sexual Assault, Burglary, Destruction of Property, Auto Theft, Kidnapping, Robbery, Fraud, Fencing of Stolen Property and Arson.

(i) Manufacturing, Use, or Possession of Explosive Devices for purposes of Homicide, Mass Murder, Fraud, Intimidation, or Political Motivation.

(j) Threats to Public Officials or Private Persons.

(k) Gang Activity.

(l) Stolen Securities.

(m) Corruption of Public Officials.

6. Source documents should identify the agency, officer, and other identifiers such as case number, arrest number, etc.

7. If open source documents were employed as part of the process of determining whether reasonable suspicion exists, copies of such documents and information that permits verification of the existence of the open source should be in the file.

8. The file should contain all available identifying information which pertains to the file subject. A non-exhaustive list would include:

(a) The full name of the person, group, association or organization.

(b) Any aliases.

(c) Any nicknames or "monikers."

(d) Date of birth or historical information.

(e) Place of birth.

(f) Citizenship or membership data.

(g) Social Security number(s).

(h) Driver's license number(s).

(i) Physical descriptors including gender and ethnicity.

(j) Distinguishing marks, scars or tattoos.

(k) FBI, CII or any other criminal history identification numbers.

(l) Evaluations of violence potential or other officer/ citizen safety information.

(m) Any other information helpful to identifying or locating the file subject. [In this connection so called "non-criminal identifying information" which relates to anyone who is not a known criminal associate should not be discoverable or searchable except as a "locator file" or "drop down" file under the name of the file subject.

(n) In no case shall files be categorized, sorted or otherwise quantified by ethnicity or gender; these factors shall only appear as factors relating to the identifying characteristics of a person. If a group, organization or association has made gender or ethnicity a determining factor in the membership or association then that characteristic of the group, organization or association may be noted in the files pertaining to that group, organization or association.

(o) In no case shall Criminal Offender Record Information (CORI) data be incorporated into the intelligence file (Title 11 CFR Section § 703). The CORI file shall be kept at a separate location from the intelligence file system.

9. All source information in the file should identify the date of submission of the information, the submitting agency and the submitting officer or employee. If the information came from a source other than law enforcement the same information should be entered except that proper considerations should be given to protect the identity of confidential informants and citizen informants.

10. Intelligence files should contain "feedback" information that allows evaluation whether the accessed/disseminated intelligence was useful or not useful, accurate or inaccurate.

(h) Intelligence file information may be made available to law enforcement officers or law enforcement agency employees who have both the "right to know" and "the need to know". The access/dissemination rules shall be the same for intelligence files as those set forth for developmental files and shall comply with the log maintenance provisions of this part.

606.7 INFORMATION CLASSIFICATION

Criminal Intelligence files should be classified to indicate the degree to which it is restricted in order to protect sources, open investigations, and to ensure the individuals rights to privacy.

(a) **Top Secret or Secret:** Highest level of security. Access limited to only those who possess the applicable federally granted Top Secret or Secret level clearance. Currently the positions who possess this clearance are the Investigation Division

Commander, Criminal Investigation Bureau Lieutenant and the Terrorism Liaison Detective.

(b) **Sensitive:** Substantial level of security. Access limited to those whose names appear on the cover sheet. Information, including, but not limited to, active police investigations, informant identification information, corruption, and those reports which require strict dissemination and release criteria.

(c) **Confidential:** Medium level of security. Access limited to Terrorism Liaison Detective / Intelligence personnel only.

(d) **Restricted:** Lowest level of security. Access limited to law enforcement personnel only. Information obtained through intelligence channels that is not classified as sensitive and is for law enforcement use only. Restricted information may include previously classified sensitive information for which the need for a high level of security no longer exists.

(e) **Unclassified:** Public Information. Information that is public in nature. This includes the following:

1. Information to which, in its original form, the general public has or had direct access (i.e., birth and death certificates).
2. News media information, such as newspaper, magazine, periodical clippings, and /or videotapes, dealing with specified criminal events.
3. Other open-source material (i.e., internet information).

606.8 DISSEMINATION /ACCESS RULES FOR CRIMINAL INTELLIGENCE FILES

(a) These files shall be accessed only on a need to know/ right to know basis in the performance of a law enforcement activity.

(b) The person directly in charge of the Intelligence Bureau and/or his/her designee shall determine who shall have access to these files.

(c) If access is granted by use of an intranet or internet connection with the authorized recipient, one of the following levels of security will be applied:

1. **Free Access:** Other parties may enter information to existing files without authorization. Other parties may not remove or alter existing information.
2. **Read-Only Access:** Other parties may see all or part of the existing information but may not enter information.
3. **"Pointer" Access:** Other parties may enter identifiers. If the result is a match to information in the file, they do not see the information, but instead are "pointed" to a contact.

(d) If intranet or internet access is not remote it shall be granted in the secure area only and the file shall not be permitted to be removed from the secure area.

(e) Any printing or copying of criminal intelligence files or any portion of criminal intelligence files shall occur only if the person in charge of the Intelligence Bureau or his/her designee approves. Both the request to print or copy and the approval shall be documented. The requesting party shall not be permitted to print or copy unless that party has demonstrated to the Hayward Police Department that that party has written policies and procedures in place which are at least as stringent as these policies and procedures. The requesting party shall agree in writing that it will not disseminate the criminal intelligence information received to a third party without notification to and consent from the Hayward Police Department.

(f) When a file is printed or copied the recipient party shall be given the discrete number assigned to that file.

(g) In all cases when there is an imminent threat of harm to persons or property and information in these files which might assist in preventing such harm shall be disseminated to persons, agencies or other entities, public or private who may be in such imminent danger or in a position to assist in preventing such harm.

606.9 PURGING OF CRIMINAL INTELLIGENCE FILES RULES

Intelligence files shall be purged from the system using the rules for purge applicable to developmental files (refer to this policy) at that point in time when they are no longer current, accurate or otherwise reliable or when five years have expired without any additional information which could support the conclusion that the subject of the file is still engaged in definable criminal activity having been added to the file.

606.10 PROCEDURE AND PROCESS REQUIREMENTS

(a) Every twelve months the Hayward Police Department developmental and intelligence files shall be audited for compliance with these policies and procedures.

(b) Specific attention shall be paid to:

1. Whether all source documents are in the file.
2. Source information has been evaluated for source and content validity.
3. Whether a purge date has been established which is current and accurate.
4. Whether procedures and processes contained within this policy are in need of updating.

(c) This audit shall be conducted by the manager in charge of the Intelligence Bureau and shall be certified by him/her as a complete and accurate audit or, if the file size is too great to be completely audited, a complete audit of a representative sample of at

least twenty (20) percent of the file shall be audited each year. When a percentage of the file only is audited a record of the control numbers of that percentage of the files shall be kept and the group of files shall not be audited again until the entire system has been audited.

(d) This audit result shall be reported to the Chief of Police.

(e) If any files are found to be out of compliance with the requirements of these policies, those files shall be withdrawn from the system of which they are part, brought into compliance and re-evaluated to determine whether they may still be maintained as part of the files system.

606.11 SPECIALIZED EQUIPMENT

The Department will make available specialized equipment to support the intelligence-gathering function. Such equipment may include night vision devices, binoculars, cameras, cellular and audiovisual equipment, and unmarked vehicles. The Criminal Investigation Bureau Lieutenant will be responsible for controlling surveillance and undercover equipment owned or used by the Department.

606.12 REVISIONS

Enacted: February 18, 2009

Revised: July 5, 2009

Revised: April 9, 2013

Revised: May 23, 2016